

BAB IV

PENGUJIAN DAN ANALISA

Pada bab ini dibahas mengenai pengujian dan hasil analisis dari konfigurasi dan simulasi yang sudah dilakukan. Seperti pada bab sebelumnya dijelaskan tujuan dari tugas ini adalah mengukur parameter *QoS* dengan *routing OSPF, EIGRP dan RIPv2*. Untuk melakukan penganalisaan dibutuhkan perangkat lunak wireshark di setiap klien dan server. *Wireshark* digunakan untuk meng-*capture* paket-paket serta *protocol* apa saja yang ada pada saat simulasi. Namun sebelum dilakukan pengukuran *QoS*, terlebih dahulu akan dilakukan pengujian terhadap konfigurasi masing-masing perangkat. apakah sudah berjalan sesuai fungsinya.

4.1 Pengujian Konfigurasi

Setelah proses instalasi dan konfigurasi pada bab sebelumnya, pada tahap ini akan dilakukan pengujian terhadap konfigurasi yang sudah dilakukan pada masing-masing perangkat. Hal ini bertujuan untuk mengetahui apakah *routing* yang dikonfigurasi sudah berjalan dengan benar dan antar perangkat sudah terkoneksi dengan baik atau belum. Adapun metode yang digunakan untuk melakukan pengujian adalah sebagai berikut:

4.1.1 Pengujian *OSPF*

Untuk mengetahui apakah *OSPF* sudah dikonfigurasi dengan benar maka dilakukan pengujian dengan melihat *routing-table* pada *core switch* dan juga melakukan tes *ping* dan *traceroute* dari client-1 ke arah *firewall*.

Pada gambar dibawah 4.1 sudah terlihat bahwa segment 192.168.1.0/24 dan segment 192.168.2.0/24 sudah masuk ke routing *OSPF* dan melalui *distribution switch* masing-masing yaitu 192.168.1.0 melalui 10.10.10.1 yang merupakan *IP interface distribution switch 2* dan segment 192.168.2.0 melalui 20.20.20.1 yang merupakan *IP interface distribution switch 1*. Hasil test ping dari klien juga sudah berhasil seperti pada gambar 4.2. pada gambar 4.1 terlihat huruf O yaitu merupakan network yang menggunakan *routing OSPF*. Salah satu diantaranya adalah segment 192.168.1.0/24 yang merupakan segment klien. Ini membuktikan bahwa klien disisi kantor pusat sudah menggunakan *routing OSPF*.

```
Core-H0#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.10.11.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/10] via 10.10.11.1, 03:40:48, Ethernet0/2
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
      C    10.10.10.0/30 is directly connected, Ethernet0/0
      L    10.10.10.2/32 is directly connected, Ethernet0/0
      C    10.10.11.0/30 is directly connected, Ethernet0/2
      L    10.10.11.2/32 is directly connected, Ethernet0/2
      O    20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
      C    20.20.20.0/30 is directly connected, Ethernet0/1
      L    20.20.20.2/32 is directly connected, Ethernet0/1
      O    90.0.0.0/32 is subnetted, 1 subnets
      O    90.90.90.1 [110/11] via 20.20.20.1, 03:45:03, Ethernet0/1
      O    100.0.0.0/32 is subnetted, 1 subnets
      C    100.100.100.10 is directly connected, Loopback0
      O    192.168.1.0/24 [110/20] via 10.10.10.1, 03:45:03, Ethernet0/0
      O    192.168.2.0/24 [110/20] via 20.20.20.1, 03:45:03, Ethernet0/1
      O    200.200.200.0/32 is subnetted, 1 subnets
      O    200.200.200.1 [110/11] via 10.10.10.1, 03:45:03, Ethernet0/0
Core-H0# sh ip ospf ne

Neighbor ID      Pri   State           Dead Time   Address        Interface
90.90.90.1       1     FULL/DR         00:00:32   20.20.20.1    Ethernet0/1
192.168.99.1     1     FULL/BDR        00:00:36   10.10.11.1    Ethernet0/2
200.200.200.1    1     FULL/DR         00:00:37   10.10.10.1    Ethernet0/0
```

Gambar 4.1 Pengujian OSPF

Pada gambar 4.2 dibawah merupakan hasil tes *ping* dari klien dengan ip 192.168.1.60 dengan tujuan 172.10.10.1 yang merupakan *IPSec* disisi *firewall* kantor sudah *reply*, ini

membuktikan bahwa dari sisi lokal disisi kantor pusat sudah berjalan sesuai konfigurasi yang sudah dilakukan.

```

root@wardani-Standard-PC-i440FX-PIIX-1996:/home/wardani# ping 172.10.10.1
PING 172.10.10.1 (172.10.10.1) 56(84) bytes of data:
64 bytes from 172.10.10.1: icmp_seq=1 ttl=253 time=2.03 ms
64 bytes from 172.10.10.1: icmp_seq=2 ttl=253 time=2.87 ms
64 bytes from 172.10.10.1: icmp_seq=3 ttl=253 time=1.84 ms
64 bytes from 172.10.10.1: icmp_seq=4 ttl=253 time=1.85 ms
64 bytes from 172.10.10.1: icmp_seq=5 ttl=253 time=1.98 ms
64 bytes from 172.10.10.1: icmp_seq=6 ttl=253 time=1.87 ms
64 bytes from 172.10.10.1: icmp_seq=7 ttl=253 time=1.77 ms
64 bytes from 172.10.10.1: icmp_seq=8 ttl=253 time=2.10 ms
^C
--- 172.10.10.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 1.771/2.042/2.877/0.337 ms

```

Gambar 4.2 Pengujian koneksi Kantor pusat

4.2.2 Pengujian *RIPv2*

Untuk mengetahui apakah *routing RIPv2* sudah dikonfigurasi dengan benar maka dilakukan pengujian dengan melihat *routing-table pada core switch* dan juga melakukan test *ping* dari klien kantor cabang A ke arah *firewall*. Pada gambar 4.3 dapat dilihat bahwa segmen 10.20.10.0/24 dan segmen 10.20.11.0/24 sudah masuk pada routing table *R* atau *RIPv2*. IP 10.20.10.0/24 melalui port ethernet 0/1 yang mengarah ke distribusi 1 dan route yang dilalui adalah 10.20.20.6 yang merupakan IP *interface* distribusi 1 yang terhubung dengan core.

```

CORE
Core-Cab-A#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is 10.20.20.1 to network 0.0.0.0

R* 0.0.0.0/0 [120/1] via 10.20.20.1, 00:00:18, Ethernet0/0
10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
R 10.20.10.0/24 [120/1] via 10.20.20.6, 00:00:09, Ethernet0/1
R 10.20.11.0/24 [120/1] via 10.20.20.10, 00:00:20, Ethernet0/2
C 10.20.20.0/30 is directly connected, Ethernet0/0
L 10.20.20.2/32 is directly connected, Ethernet0/0
C 10.20.20.4/30 is directly connected, Ethernet0/1
L 10.20.20.5/32 is directly connected, Ethernet0/1
C 10.20.20.8/30 is directly connected, Ethernet0/2
L 10.20.20.9/32 is directly connected, Ethernet0/2
Core-Cab-A#

```

Gambar 4.3 Hasil pengujian *RIPv2*

Pada gambar 4.4 dibawah merupakan hasil tes ping dari klien dengan IP 10.20.11.11 ke ip 172.10.10.10 yang merupakan IPSec disisi firewall kantor cabang A. dari pengetesan tersebut membuktikan bahwa dari sisi lokal disisi kantor cabang A sudah berjalan sesuai konfigurasi.

```

cabang-a@cabanga-Standard-PC-l440FX-PIIX-1996:~$ ping 172.10.10.10
PING 172.10.10.10 (172.10.10.10) 56(84) bytes of data.
64 bytes from 172.10.10.10: icmp_seq=1 ttl=254 time=2.39 ms
64 bytes from 172.10.10.10: icmp_seq=2 ttl=254 time=2.08 ms
64 bytes from 172.10.10.10: icmp_seq=3 ttl=254 time=2.07 ms
64 bytes from 172.10.10.10: icmp_seq=4 ttl=254 time=1.96 ms
64 bytes from 172.10.10.10: icmp_seq=5 ttl=254 time=2.04 ms
64 bytes from 172.10.10.10: icmp_seq=6 ttl=254 time=1.92 ms
64 bytes from 172.10.10.10: icmp_seq=7 ttl=254 time=1.86 ms
64 bytes from 172.10.10.10: icmp_seq=8 ttl=254 time=2.26 ms
64 bytes from 172.10.10.10: icmp_seq=9 ttl=254 time=2.56 ms
64 bytes from 172.10.10.10: icmp_seq=10 ttl=254 time=2.19 ms
64 bytes from 172.10.10.10: icmp_seq=11 ttl=254 time=2.28 ms
64 bytes from 172.10.10.10: icmp_seq=12 ttl=254 time=1.97 ms
64 bytes from 172.10.10.10: icmp_seq=13 ttl=254 time=2.03 ms
64 bytes from 172.10.10.10: icmp_seq=14 ttl=254 time=2.14 ms
^C
--- 172.10.10.10 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13017ms
rtt min/avg/max/mdev = 1.860/2.128/2.560/0.195 ms

```

Gambar 4.4 Pengujian koneksi kantor cabang A

4.2.3 Pengujian *EIGRP*

Untuk mengetahui apakah *routing EIGRP* sudah dikonfigurasi dengan benar maka dilakukan pengujian dengan melihat *routing-table pada core switch* dan juga melakukan test *ping* dari klien kantor cabang A ke arah *firewall*. Pada gambar 4.5 dapat dilihat bahwa segmen 10.30.10.0/24 dan segmen 10.30.11.0/24 sudah masuk pada ip *protocol EIGRP*. IP klien dengan segment 10.30.11.11/24 akan melalui distribusi switch 1, kemudian diteruskan dengan vlan 20 melalui *switch akses*. *EIGRP* merupakan routing yang hanya bisa digunakan pada perangkat cisco, *sehingga* interface ke arah *firewall fortigate* menggunakan *static route*. Dimana default route atau tujuan dengan IP berapapun akan dialirkan ke arah *firewall fortigate*, kecuali IP disisi klien distribusi 2,

```

R1#show ip protocols

Routing Protocol is "eigrp 1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    10.0.0.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170

R1#

```

Gambar 4.5 Pengujian EIGRP

Pada gambar 4.6 merupakan hasil pengujian koneksi pada kantor cabang B, dimana tes Ping dari klient ke arah IP 172.10.10.11 yang merupakan ip disisi firewall kantor cabang B sudah reply. pengetesan tersebut membuktikan bahwa dari sisi lokal disisi kantor cabang B sudah berjalan sesuai konfigurasi.

```

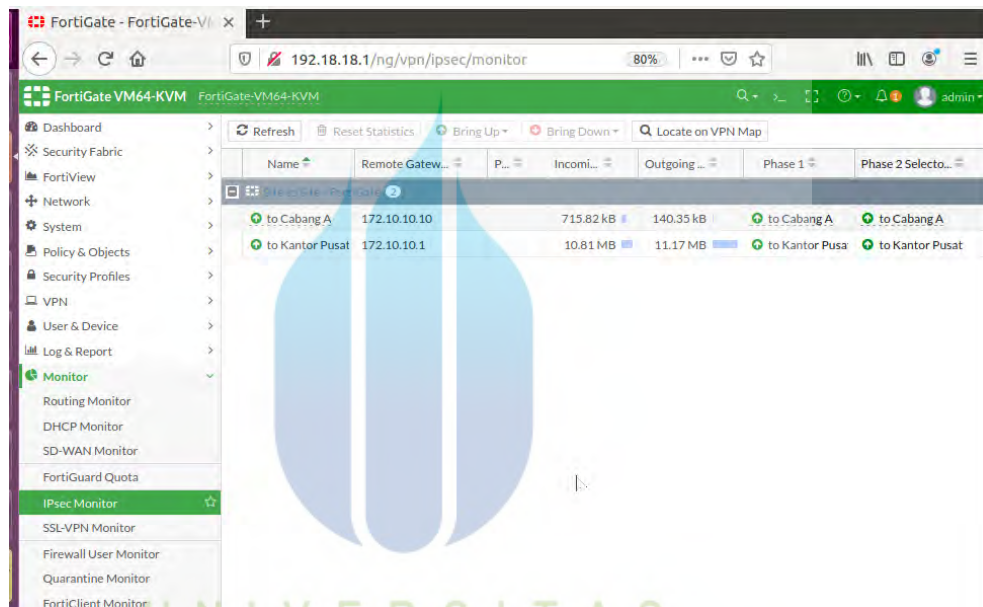
client-voip@clientvoip-Standard-PC-i440FX-PIIX-1996:~$ ping 172.10.10.11
PING 172.10.10.11 (172.10.10.11) 56(84) bytes of data:
64 bytes from 172.10.10.11: icmp_seq=1 ttl=253 time=1.51 ms
64 bytes from 172.10.10.11: icmp_seq=2 ttl=253 time=1.65 ms
64 bytes from 172.10.10.11: icmp_seq=3 ttl=253 time=1.57 ms
64 bytes from 172.10.10.11: icmp_seq=4 ttl=253 time=1.59 ms
64 bytes from 172.10.10.11: icmp_seq=5 ttl=253 time=1.33 ms
64 bytes from 172.10.10.11: icmp_seq=6 ttl=253 time=1.54 ms
64 bytes from 172.10.10.11: icmp_seq=7 ttl=253 time=1.47 ms
64 bytes from 172.10.10.11: icmp_seq=8 ttl=253 time=1.56 ms
64 bytes from 172.10.10.11: icmp_seq=9 ttl=253 time=1.44 ms
64 bytes from 172.10.10.11: icmp_seq=10 ttl=253 time=1.49 ms
64 bytes from 172.10.10.11: icmp_seq=11 ttl=253 time=1.57 ms
64 bytes from 172.10.10.11: icmp_seq=12 ttl=253 time=1.54 ms
64 bytes from 172.10.10.11: icmp_seq=13 ttl=253 time=1.48 ms
64 bytes from 172.10.10.11: icmp_seq=14 ttl=253 time=1.55 ms
^C
--- 172.10.10.11 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13015ms
rtt min/avg/max/mdev = 1.339/1.526/1.652/0.080 ms
client-voip@clientvoip-Standard-PC-i440FX-PIIX-1996:~$

```

Gambar 4.5 Pengujian koneksi kantor cabang B

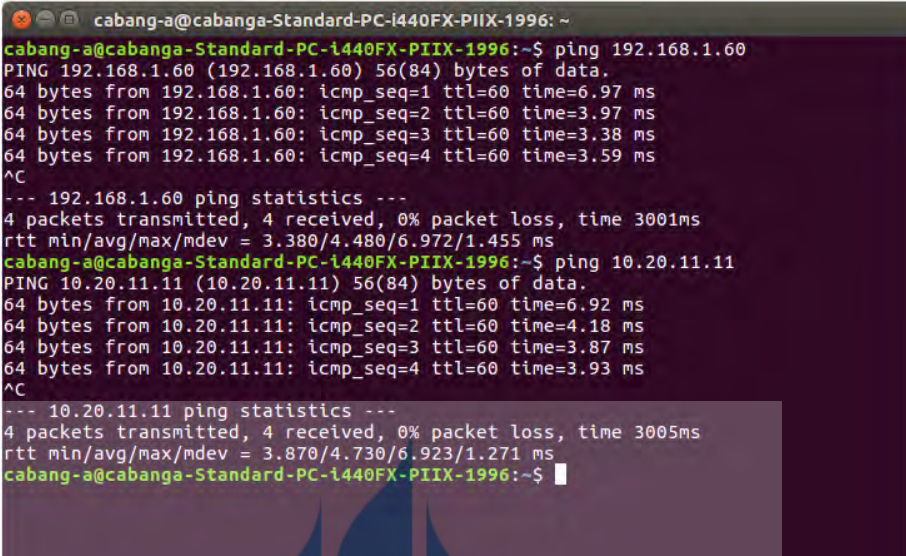
4.3.3 Pengujian VPN IPsec

Pengujian VPN IPsec bertujuan untuk mengetahui apakah VPN sudah dikonfigurasi dengan benar dan VPN IPsec sudah *establish*. Untuk mengetahuinya dapat dilihat pada *Firewall Fortigate di data center*. Pada menu monitor lalu pilih IPsec VPN seperti gambar 4.5 dibawah.



Gambar 4.7 Pengujian VPN IPsec Tunnels

Selanjutnya pengujian kedua dengan melakukan tes *ping* dari data center ke klien di kantor pusat dan kantor cabang. Hal ini bertujuan untuk memastikan koneksi dari data center atau server ke kantor pusat dan kantor cabang sudah terhubung. Gambar 4.6 dibawah menunjukkan bahwa koneksi sudah berhasil.



```

cabang-a@cabanga-Standard-PC-i440FX-PIIX-1996: ~
cabang-a@cabanga-Standard-PC-i440FX-PIIX-1996:~$ ping 192.168.1.60
PING 192.168.1.60 (192.168.1.60) 56(84) bytes of data.
64 bytes from 192.168.1.60: icmp_seq=1 ttl=60 time=6.97 ms
64 bytes from 192.168.1.60: icmp_seq=2 ttl=60 time=3.97 ms
64 bytes from 192.168.1.60: icmp_seq=3 ttl=60 time=3.38 ms
64 bytes from 192.168.1.60: icmp_seq=4 ttl=60 time=3.59 ms
^C
--- 192.168.1.60 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 3.380/4.480/6.972/1.455 ms
cabang-a@cabanga-Standard-PC-i440FX-PIIX-1996:~$ ping 10.20.11.11
PING 10.20.11.11 (10.20.11.11) 56(84) bytes of data.
64 bytes from 10.20.11.11: icmp_seq=1 ttl=60 time=6.92 ms
64 bytes from 10.20.11.11: icmp_seq=2 ttl=60 time=4.18 ms
64 bytes from 10.20.11.11: icmp_seq=3 ttl=60 time=3.87 ms
64 bytes from 10.20.11.11: icmp_seq=4 ttl=60 time=3.93 ms
^C
--- 10.20.11.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 3.870/4.730/6.923/1.271 ms
cabang-a@cabanga-Standard-PC-i440FX-PIIX-1996:~$

```

Gambar 4.8 Test Ping Data center ke site

4.2 Pengukuran dan Analisa Performansi

Setelah dilakukan pengukuran pada *video conference* menggunakan Wireshark, maka akan dilakukan analisis performansi untuk mengetahui kelayakan *server routing* yang terintegrasi dengan VPN yang telah ditentukan menggunakan scenario dari perancangan sistem. Pengukuran dilakukan pada setiap klien dan pada *server*, dari setiap klien memiliki *bandwidth* dan *throughput* yang berbeda-beda. Ini bertujuan untuk mengetahui kelayakan dari *routing* tersebut dengan menggunakan standar ITU-T.

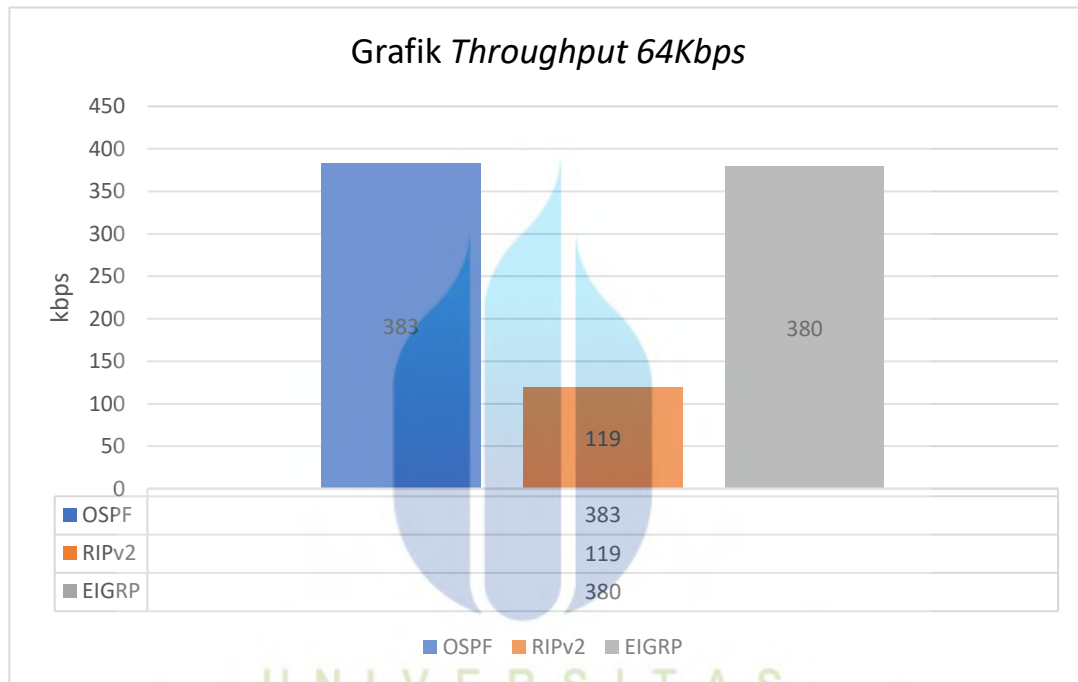
4.2.1 Pengukuran dan Analisis *Throughput*

Throughput merupakan jumlah *bit* yang sukses dikirimkan dari pengirim ke penerima. Pengukuran pada layanan *VoIP* digunakan untuk mengetahui atau menilai kehandalan dari layanan *Voip* dalam mengirimkan paket ke klien yang sedang melakukan panggilan. pengukuran dilakukan dengan melakukan interkoneksi antara server *asterisk* di *Data Center* dengan kantor pusat dan kantor cabang A. Setelah berhasil melakukan panggilan dan selama panggilan berlangsung semua komunikasi di *capture* menggunakan *network analyzer* yaitu Wireshark. Pengukuran dilakukan

dengan durasi 5 menit panggilan. Kemudian dapat melihat hasilnya pada *statistic* dan *summary*. Adapun hasil dari pengukurannya seperti gambar dibawah.

1. Pengukuran *throughput* dengan bandwidth 64 Kbps

Pada pengujian dengan bandwidth 64 Kbps diperoleh hasil sebagai berikut:

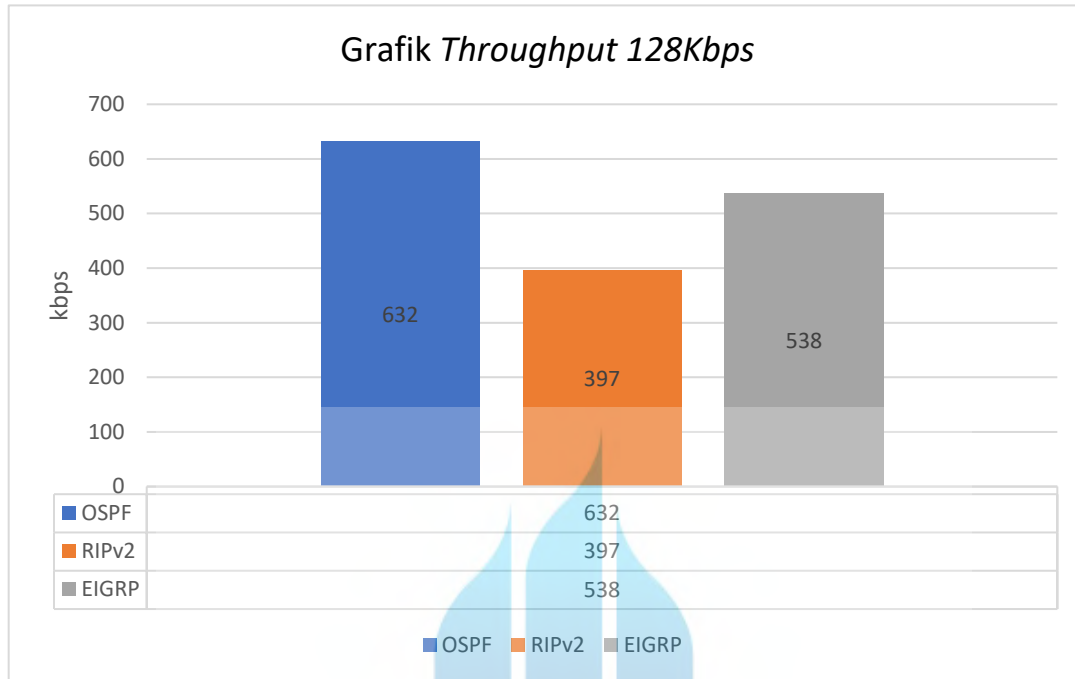


Gambar 4.8 Grafik *Throughput* 64Kbps

Hasil pengukuran pada *bandwidth* 64 KBps yang terlihat pada gambar 4.2 *throughput* yang didapat pada klien kantor pusat dengan routing OSPF adalah sebesar 382 kbps dan hasil yang didapat untuk klien kantor cabang A dengan routing RIPv2 adalah 119 kbps dan di kantor cabang B dengan routing EIGRP adalah 380 kbps.

2. Pengukuran *throughput* dengan bandwidth 128 Kbps

Pada pengujian dengan bandwidth 128 Kbps diperoleh hasil sebagai berikut:

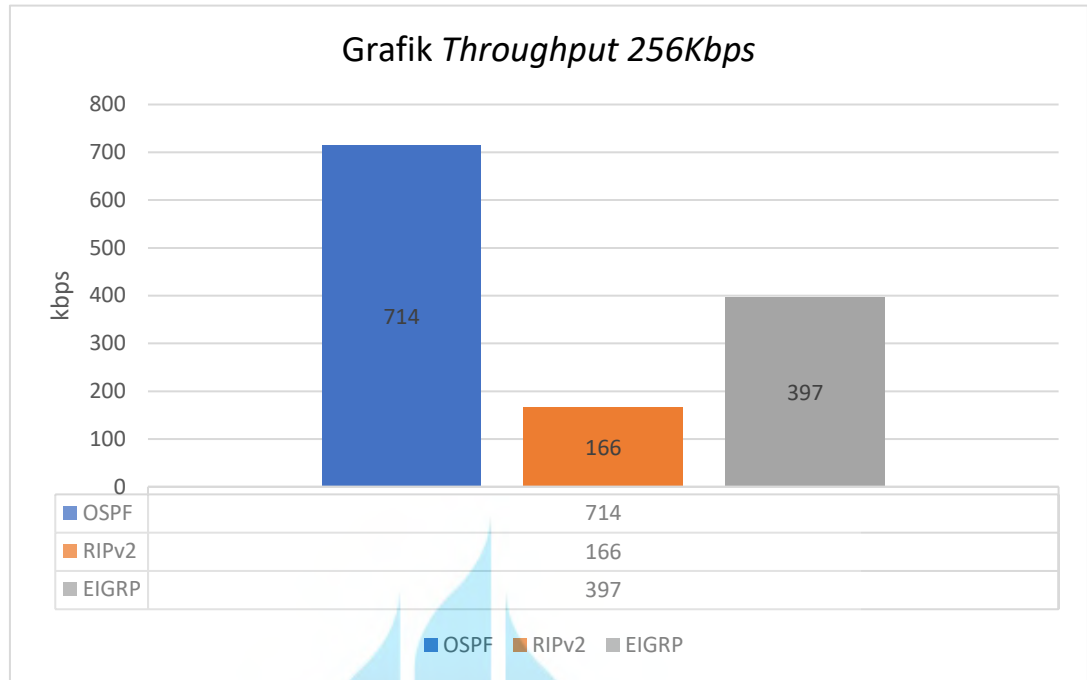


Gambar 4.9 Grafik *Throughput 128Kbps*

Hasil pengukuran pada *bandwidth* 128 Kbps yang terlihat pada gambar 4.2 *throughput* yang didapat pada klien kantor pusat dengan routing OSPF adalah sebesar 632 kbps dan hasil yang didapat untuk klien kantor cabang A dengan routing RIPv2 adalah 397 kbps dan di kantor cabang B dengan routing EIGRP adalah 538 kbps.

3. Pengukuran *throughput* dengan bandwidth 256 Kbps

Pada pengujian dengan bandwidth 256 Kbps diperoleh hasil sebagai berikut:



Gambar 4.10 Grafik Troughput 256Kbps

Hasil pengukuran pada *bandwidth* 256 Kbps yang terlihat pada gambar 4.2 *throughput* yang didapat pada klien kantor pusat dengan routing OSPF adalah sebesar 714 kbps dan hasil yang didapat untuk klien kantor cabang A dengan routing RIPv2 adalah 166 kbps dan di kantor cabang B dengan routing EIGRP adalah 397 kbps.

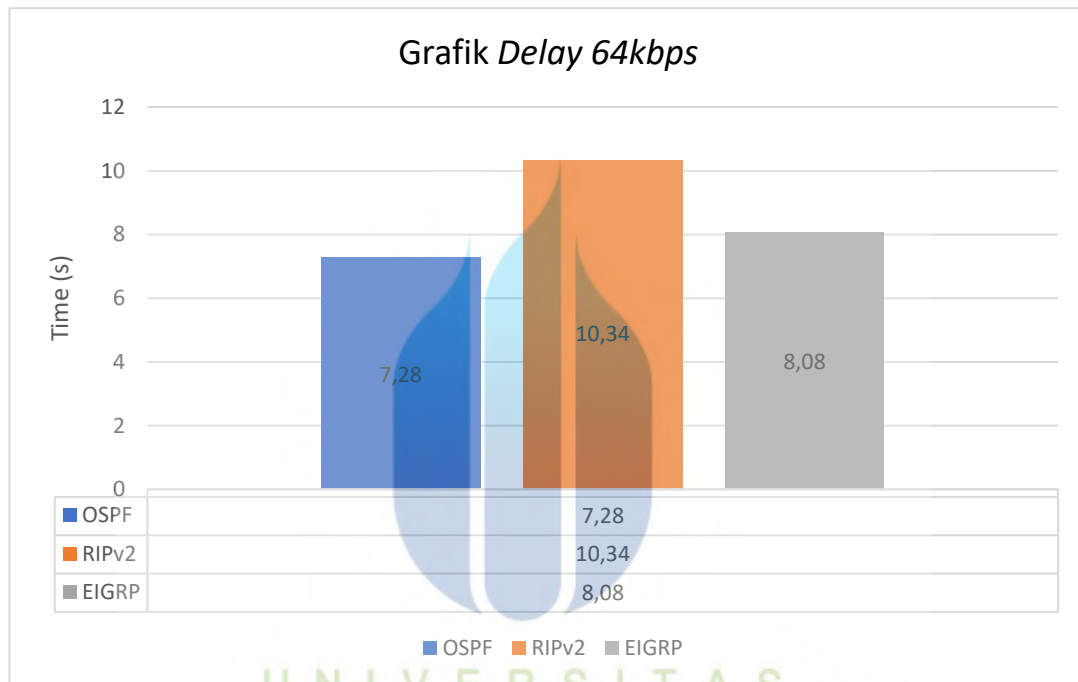
4.2.2 Pengukuran dan Analisis Delay

Delay adalah waktu yang dibutuhkan sebuah paket ketika dikirim antara pengirim ke penerima. Secara umum *delay* yang terukur oleh Wireshark adalah *interrival delay*. Besar kecilnya suatu *delay* sangat berpengaruh pada performansi jaringan yang dapat dirasakan oleh *end user*. Pengukuran dilakukan dengan melakukan interkoneksi klien pada kantor cabang A ke *server data center*. Semua komunikasi di *capture* menggunakan *network analyzer* yaitu Wireshark. Pengukuran dilakukan dengan interval waktu 5 menit panggilan. Skenario pengukuran dilakukan dengan cara mengukur *delay* yang didapat di sisi klien-klien yang telah terhubung. Setelah berhasil melakukan panggilan dan selama panggilan berlangsung semua komunikasi di *capture* menggunakan *network analyzer* yaitu Wireshark. Pada aplikasi wireshark dapat dilihat

pada menu *Telephony*, pilih RTP kemudian *Show All Stream* pilih *Stream Analysis* pilih *IP klien* dan Pilih *Analyze*. Hasilnya dapat dilihat pada gambar dibawah.

1. Pengukuran *Delay* dengan bandwidth 64 Kbps

Pada pengujian dengan bandwidth 64 Kbps diperoleh hasil sebagai berikut:

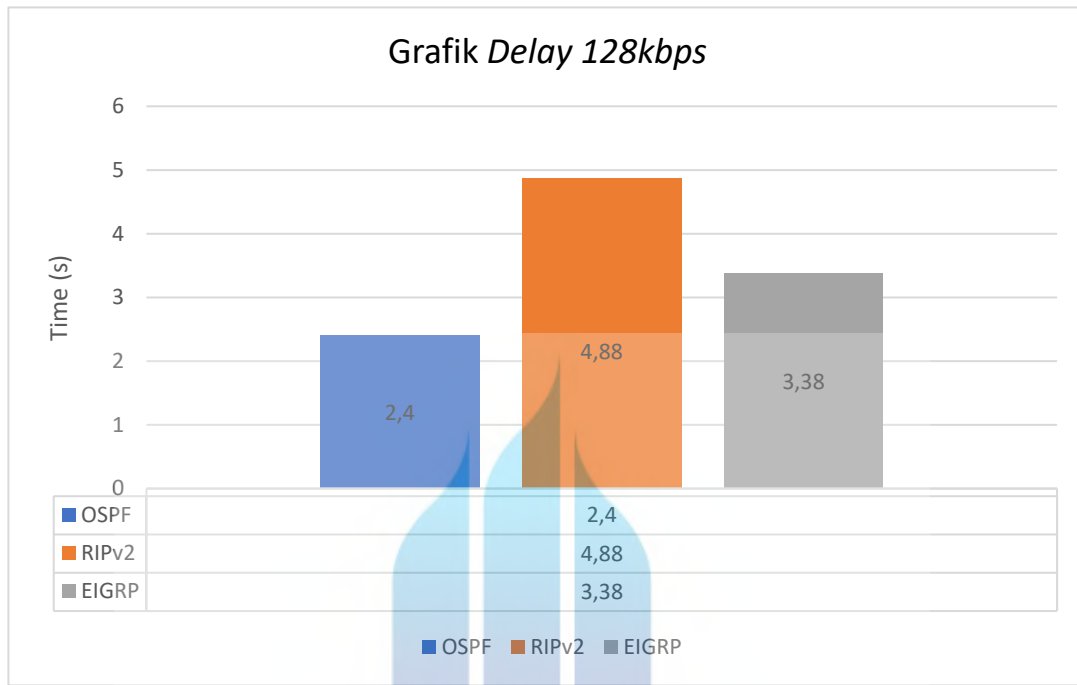


Gambar 4.11 Grafik Delay 64Kbps

Hasil pengukuran *Delay badwidth 64 Kbps* yang terlihat pada gambar 4.8 yang didapat pada client kantor pusat dengan *routing OSPF* adalah sebesar 7,28 s dan hasil yang didapat untuk client kantor cabang A dengan *routing RIPv2* adalah 10,34 s, pada kantor cabang B diperoleh hasil 8.08s. Dari pengukuran yang sudah dilakukan hasilnya sudah memenuhi standar yang ditentukan ITU-T yaitu delay kurang dari 150 s.

2. Pengukuran *throughput* dengan bandwidth 128 Kbps

Pada pengujian dengan bandwidth 128 Kbps diperoleh hasil sebagai berikut:

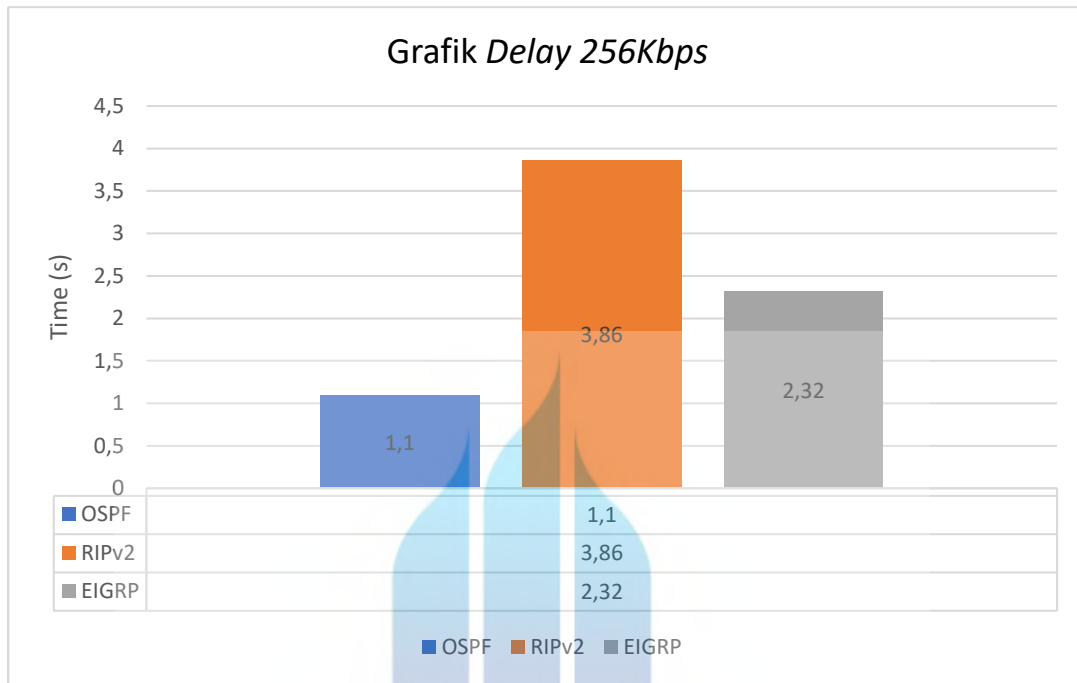


Gambar 4.12 Grafik Delay 128 Kbps

Hasil pengukuran *Delay badwidth 128 KBps* yang terlihat pada gambar 4. yang didapat pada client kantor pusat dengan *routing OSPF* adalah sebesar 2,4 s dan hasil yang didapat untuk client kantor cabang A dengan *routing RIPv2* adalah 4,88 s, pada kantor cabang B diperoleh hasil 3,38s. Dari pengukuran yang sudah dilakukan hasilnya sudah memenuhi standar yang ditentukan ITU-T yaitu delay kurang dari 150 s.

3. Pengukuran *troughput* dengan bandwidth 256 Kbps

Dari hasil pengukuran *Delay badwidth 256 KBps* yang terlihat pada gambar 4. yang didapat pada client kantor pusat dengan *routing OSPF* adalah sebesar 1,1 s dan hasil yang didapat untuk client kantor cabang A dengan *routing RIPv2* adalah 3,86 s, pada kantor cabang B diperoleh hasil 2,32s. Dari pengukuran yang sudah dilakukan hasilnya sudah memenuhi standar yang ditentukan ITU-T yaitu delay kurang dari 150 s.



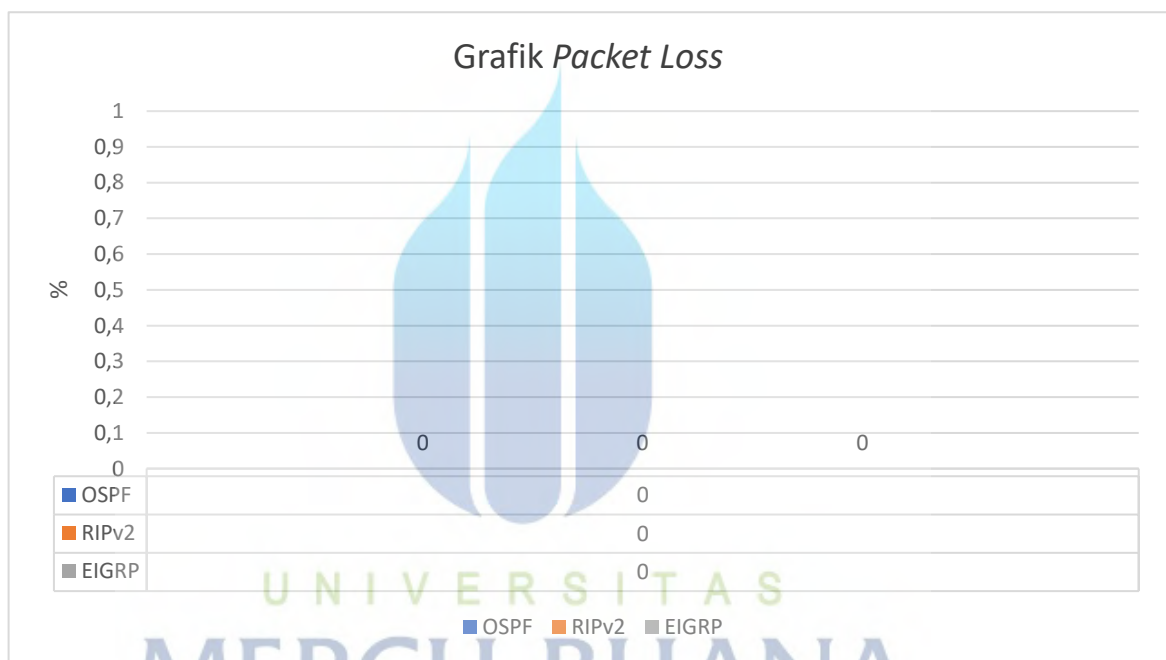
Gambar 4.13 Grafik Delay 128 Kbps

Dari ketiga pengukuran diatas hasilnya sudah sesuai standar yang ditentukan ITU-T yaitu delay kurang dari 150s. adapun pengaruh *bandwidth* terhadap layanan yang diberikan adalah semakin besar *bandwidth* yang diberikan maka akan semakin baik kualitas jaringan tersebut.

4.2.3 Pengukuran dan Analisis *Packet Loss*

Pengukuran *packet loss* bertujuan untuk mengetahui kehandalan dari sistem yang telah dibuat. Banyaknya data yang dikirim dan diterima akan mempengaruhi kualitas layanan tersebut, oleh karena itu pengukuran *packet loss* bertujuan untuk mengetahui presentasi banyaknya paket yang gagal mencapai tujuan pada saat pengiriman paket. Pengukuran dilakukan dengan melakukan interkoneksi seluruh klien ke *server Asterik* dengan menggunakan perangkat lunak *twinkle* disisi klien yang selanjutnya akan melakukan panggilan. Setelah semua terkoneksi maka klien dapat melakukan panggilan dan selama panggilan berlangsung semua komunikasi di *capture*

menggunakan *network analyzer* yaitu Wireshark. Skenario pengukuran dilakukan dengan cara mengukur antara *packet loss* yang diterima di sisi klien. Setelah itu dapat dilihat *packet loss* pada *statistic* ke *summary*, adapun hasil pengukurannya adalah tidak ditemukan adanya *paket loss* baik dengan *routing OSPF* maupun pada *routing RIPv2* dan *EIGRP* pada bandwidth 64Kbps, 128 Kbps dan 256 Kbps.



Gambar 4.14 Grafik Packet Loss

4.2.4 Hasil Pengukuran Keseluruhan

Dari pengukuran yang sudah dilakukan diatas berikut ini merupakan rangkuman dari hasil pengukuran :

Tabel 4.1 Hasil pengukuran *QoS*

<i>Bandwidth</i>	<i>Throughput</i> (Kbps)	<i>Packet loss</i> (%)	<i>Delay</i> (s)	keterangan
64	383	0	7,28	<i>OSPF</i> (Kantor Pusat)
128	632	0	2,4	
256	714	0	1,1	
64	119	0	10,34	<i>RIPv2</i> (Kantor Cabang A)
128	397	0	4,88	
256	166	0	3,86	
64	380	0	8,08	<i>EIGRP</i> (kantor cabang B)
128	538	0	3,38	
256	397	0	2,32	

Dari hasil pengukuran pada table 4.1 diatas dapat dijelaskan bahwa pengukuran pada masing-masing *routing* sudah sesuai dengan standar ITU-T, yaitu paket loss kurang dari 1% dan delay kurang dari 50 *second*. Dari table tersebut juga dapat dilihat bahwa *bandwidth* berpengaruh terhadap *QoS*, pada pengujian dengan *routing OSPF*, *RIPv2* maupun *EIGRP* terlihat bahwa semakin besar *bandwidth* yang diberikan maka akan semakin baik kualitas dari sebuah jaringan tersebut, ini dapat dilihat pada *delay* yang semakin kecil dan *troughput* yang semakin baik pada *bandwidth* yang lebih besar. Pada pengujian yang sudah dilakukan terlihat bahwa *routing* dengan kualitas yang paling baik adalah dengan *routing OSPF*.